REMARKS

Claims 18-28, and 41-59 are in the application.

Claims 22-28 are withdrawn from consideration as being directed to non-elected inventions, and will be rejoined with the application if claim 21 is deemed allowable.

Claims 1-17 and 29-40 are cancelled without prejudice or disclaimer as being directed to a non-elected invention.

Claims 18-21 and 41-45 are subject to examination.

Claim 42 is amended to depend from new claim 46, which is similar in form to claim 18, but which employs the phrase "cryptographically processed" instead of "hash". It is believed that claims 41-42, and 46-59, lie within the elected group.

The Examiner states that "Li discloses an optical recording media having optically variable security properties (see abstract and Fig. 1). In Fig. 26 Li show[] the pattern applied to the recording medium. Li teaches that the position of the reflection peaks (i.e. pattern) depends on phase thickness, which is given by equation 1 (see column 6). Equation [] produces a cipher, which defines the pattern on the recording medium. The produced cipher meets the limitation 'hash being formed from a respective data pattern'. Li, however, does not explicitly teach that the data pattern is created on the disc in the form of a random fiber or molded pattern."

Claim 18 requires:

An optically readable data storage medium, comprising

an optically readable substrate having a data pattern and a set of optically readable characteristics which are randomly determined by a non-deterministic physical manufacturing process,

further comprising a recorded hash of identifications ["a cryptographically processed set of identifications" in claim 46] of the random optically readable characteristics and the data pattern associated with the data storage medium,

the data pattern and the optically readable characteristics being adapted to be readable by a common imaging system,

wherein the data storage medium is resistant to reproduction and alteration of the data pattern can be detected.

Claim 43 requires:

An optically readable data storage medium, comprising:

an adhesive-backed flexible substrate;

periodically disposed sets of optically readable data patterns on said substrate;

regions of said substrate having optically readable characteristics which are randomly determined by a non-deterministic physical manufacturing process proximate to a respective data pattern; and

periodically disposed sets of recorded hashes, each respective hash being formed from a respective data pattern and characteristics of a respective region,

wherein the data storage medium is resistant to reproduction and alteration of the data pattern can be detected.

It is conceded that Li discloses an optically readable data storage medium, which has (or is modified to have) a data pattern or data patterns. The medium of Li is also apparently resistant to reproduction.

Li does not disclose an adhesive-backed flexible substrate (per claim 43).

Li does not teach or suggest optically readable characteristics which are randomly determined by a non-deterministic physical manufacturing process. The thin film structures of Li are each presumably manufactured to precise optical specifications to avoid random effects, and therefore to permit use of the various nominal formulae as expressing the characteristics of the medium.

Applicants' undersigned attorney can find no teaching or suggestion, or even a hint, of derivation or use a "cipher" in Li. "Cipher" and "Hash" are defined as (contextually inappropriate definitions excluded):

http://www.google.com/search?sourceid=navclient&ie=UTF-8&rls=GGLG,GGLG:2005-25,GGLG:en&q=define%3A+cipher

- encode: convert ordinary language into code; "We should encode the message for security reasons"
- a secret method of writing
- calculate: make a mathematical calculation or computation
  wordnet.princeton.edu/perl/webwn
- In cryptography, encryption is the process of obscuring information to make it unreadable without special knowledge. While encryption has been used to protect communications for centuries, only organisations and individuals with an extraordinary need for secrecy have made use of it. ...
  en.wikipedia.org/wiki/CipheR
- In Cryptographic Support, data that is unintelligible to all except those who have the key to decode it to plaintext.
  www.sabc.co.za/manual/ibm/9agloss.htm

- a cryptographic algorithm used to encrypt and decrypt files and messages.
  www.cdt.org/crypto/glossary.shtml
- The method used to transform a readable message (called plaintext or cleartext) into an unreadable, scrambled or hidden message (called ciphertext).
  www.microsoft.com/security/glossary.mspx
- A cryptographic algorithm, ie a mathematical function used for encryption and decryption.
  www.efa.org.au/Issues/Crypto/crypto5.html
- 1. A method of transforming texts character by character in order to conceal their meaning. 2. Such transformed messages.
  www.csa.com/hottopics/crypt/gloss.php
- Any encryption algorithm. Ciphers can be classified according to whether they are symmetric or public key algorithms, and by whether they operate on their data as a stream or divided into blocks.
  survey.netcraft.com/surveys/analysis/https/2004/Jan/glossary.html
- a secret way of writing (way of encrypting)
  www-fs.informatik.uni-tuebingen.de/~reinhard/krypto/English/1.1.e.html
- An algorithm for encryption or decryption. A cipher replaces a piece of information (an element of plain text) with another object, with the intent to conceal meaning. Typically, the replacement rule is governed by a secret key.
  www.primode.com/glossary.html
- Key to a secret, as in a geometric secret, for example.
  unistates.com/rmt/explained/glossary/rmtglossaryc.html
- A cryptographic transformation that operates on characters or bits.
  library.ahima.org/xpedio/groups/public/documents/ahima/pub_bok1_021589.html
- A secret representation of plain language, consisting of groups of letters and/or figures, normally 4 or 5 to a group.
  www.airbornerecce.com/dtroop/RSigs/sigterm.htm
- a formal coded message where its original meaning has been obscured
  www.open.ac.uk/learning/induction/undergraduate/studytips/glossary-example-t209.htm.
- An arithmetical character, used for numerical notation. Vide Figures, and 13 Vin. Ab. 210; 18 Eng. CLR 95; 1 Ch. Cr. Law, 176.
  www.new-york-lawyer.ws/law-dictionary/chemistry.htm
- In cryptography, the word cipher means an encryption algorithm. A cipher transforms the original data/message into pseudo-random data/message of the same length. In order to decipher the message, a reverse transformation must be applied.
  secwatch.org/glossary/terms/C

A hash is defined as:

http://www.google.com/search?sourceid=navclient&ie=UTF-8&rls=GGLG,GGLG:2005-25,GGLG:en&q=define%3A+hash

- Producing hash values for accessing data or for security. A hash value (or simply hash), also called a message digest, is a number generated from a string of text. The hash is substantially smaller than the text itself, and is generated by a formula in such a way that it is extremely unlikely that some other text will produce the same hash value.
  www.cscic.state.ny.us/msisac/webcasts/6_04/6_22_terms.htm
- A short value calculated from digital data that serves to distinguish it from other data.
  www.cs.cornell.edu/wya/DigLib/MS1999/glossary.html
- Data allocated in an algorithmically randomized fashion in an attempt to evenly distribute data and smooth access patterns.
  www.dmreview.com/resources/glossary.cfm

- A number generated by applying a mathematical formula to a document or sequence of text. The hash is significantly shorter that the original text and is unique to the original document. www.epa.gov/cdx/about/glossary.htm
- A hash function is a computationally efficient function mapping binary strings or arbitrary length to binary strings of some fixed length, called hash-values. ... www.wetstonetech.com/page/page/1972572.htm
- A one-way algorithm which maps or translates one set of bits into another (generally smaller) in such a way that the algorithm yields the same hash results every time for the same message, and it is computationally infeasible for a message to be reconstituted from the hash result. Also, two different messages cannot produce the same hash results. www.infosec.gov.hk/english/general/glossary_gj.htm
- A fixed-length value created mathematically to uniquely identify data. www.cafesoft.com/support/security-glossary.html
- A mathematical computation that takes a variable-size message and returns a fixed-size string to authenticate (prove the integrity) of a message. Examples are SHA and M5. A component of IKE, IPsec and digital signatures. Top www.sequi.com/SEQUI_VPN_Glossary.htm
- Value resulting from invoking a Hash Function. Also called a Digest. www.orionsec.com/Security_Glossary.html
- A collection of data in which each piece of data has two components, a key and a value; also called an associative array. www.metromemetics.com/thelexicon/h.asp
- A function that takes a variable-length input and produces a fixed-length output. www.lancs.ac.uk/postgrad/grech/glossaryh.htm
- message digest www.smartcard.co.uk/glossary.html

With all due respect, applicants' review of Li fails to discover any discussion of ciphers, hashes, and random patterns, at all. While the examiner states that "Equation [] produces a cipher", he provides no basis of support for this allegation, nor any clear indication that an appropriate definition of cipher is being employed. **Applicants respectfully request clarification by the Examiner and a specific reference to Figure number, or column and line, where the Examiner draws the conclusion that a cipher is produced.** To the extent that the Examiner implies that the normal encoding of bits on the recording medium is a "cipher", it is noted that the disclosure of Li fails to indicate any "secret", key, or special knowledge, a required element of a cipher.

The Examiner extends this unsupported inference, by stating: "The produced cipher meets the limitation 'hash being formed from a respective data pattern.'" The Examiner thus equates the cipher and hash. While applicants admit that hashes and ciphers are related in the field of cryptography, applicants find no disclosure of any cryptographic techniques in Li. Typically, a cipher is a reversible function (two way), while a hash is not (one way), and therefore the Examiners' analysis equating these two concepts is flawed at this second level as

well. **Applicants respectfully request clarification by the Examiner and a specific reference to Figure number, or column and line, where the Examiner draws the conclusion that a hash is produced.**

The pattern on the recording medium is defined independently of the medium, and there is simply no disclosure, teaching or suggestion that the data pattern recorded on the medium is dependent on aspects of the medium itself, which differ from medium to medium, that is, differ based on "a set of optically readable characteristics which are randomly determined by a non-deterministic physical manufacturing process". The security features of Li are apparently limited to "optically-variable properties", i.e., "producing a color shift with a change of viewing angle..." Li, Col. 2, lines 14-18. Li simply states: "The information is encoded by photolithographic means or by optical recording means." (Abstract).

Claim 18, in particular, requires "a recorded hash of identifications of the random optically readable characteristics and the data pattern associated with the data storage medium." Claim 43 requires "periodically disposed sets of recorded hashes, each respective hash being formed from a respective data pattern and characteristics of a respective region". Claim 46 requires "a cryptographically processed set of identifications of the random optically readable characteristics and the data pattern associated with the data storage medium". Each of these is clearly absent from Li.

A review of Li does not clearly indicate that alteration of the data pattern can be detected, and indeed, erasable media are disclosed (Col. 2, line 10) such that this is not an inherent property of Li's invention.

The Examiner cites Waters for the proposition that is was known to serialize a disc by physically damaging a portion to create a pattern of damage, which is then encoded on the disc. This renders the disc somewhat resistant to normal reproduction, though it appears that the very technique taught by the patent, using a similar device to that used by an authorized publisher to protect is own content, could be used to duplicate a disk with an identical code and identical damage pattern. Thus, it is not clear that Waters meets this claim limitation. However, we assume arguendo that the difficulty in obtaining the device that is presumably taught and enabled by Waters qualifies as "resistant to reproduction".

The damage to the disk of Waters is not random, and is intentionally produced at predetermined locations on the disk, thus rendering the damage deterministic. Likewise, the

damage pattern is produced according to in an "identifying value", which is then encrypted (alone, or with other data) and written on the disc. While this "identifying value" is encrypted, it is not apparent that it represents a hash.

Neither Li nor Waters teaches or suggests a disc or other medium having a fiber pattern. The Examiner states: "Therefore, at the tine the invention was made, it would have been obvious to one of ordinary skill in the art to create the optical recording media having optically variable properties of Li, by damaging (i.e. changing) the fiber pattern of the optical disk as taught by Wa[]ters. One of ordinary skill in the art would have been motivated to create the optical recording media having optically variable properties of Li, by changing the fiber pattern of the optical disc as taught by Wa[]ters for authenticating the disc based on the pattern (see Wa[]ters, column 1, lines 25-35 and Fig. 9)." With all due respect, Waters et al. does not teach or suggest the use of fibers, or any kind, and thus the argument bootstraps the inferred disclosure of fibers in Waters et al. to an otherwise unsupported allegation of obviousness. **Applicants respectfully request clarification by the Examiner and a specific reference to Figure number, or column and line, where the Examiner draws the conclusion that a fiber pattern is taught by Waters et al.**

Claim 21 requires:

A data storage disk, comprising

a graphic-bearing surface,

a code printed on the graphic bearing surface, and

an ascertainable pattern formed during a physical non-deterministic manufacturing process formed on the disk,

wherein the printed code provides self authentication for the disk based on the ascertainable pattern,

the printed code and the ascertainable pattern being adapted to be readable by a common imaging system, wherein the data storage disk is resistant to reproduction.

Waters et al. discloses a data storage disk having a graphic bearing surface, with a printed code thereon, which is used for self-authentication of the disk. Neither Li nor Waters et al., as discussed above, teach or suggest that "an ascertainable pattern [is] formed during a physical non-deterministic manufacturing process formed on the disk," and are thus distinguished.

Further, the printed code of Waters et al. is human readable, and is not particularly intended to be read by the same system that reads the data recorded on the disk.

It is therefore respectfully submitted that the present claims are patentable, and a Notice of Allowance is respectfully solicited.

Respectfully submitted,
MILDE & HOFFBERG, LLP

By
Steven M. Hoffberg
Reg. No. 33,511

MILDE & HOFFBERG, LLP
10 Bank Street - Suite 460
White Plains, NY 10606

914-949-3100